

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented): A computer implemented method for validating a user's authorization to run a tool in a service control manager (SCM) module by a security manager, comprising:

creating a runnable tool, wherein the runnable tool encapsulates a tool and includes a tool definition and a list of target nodes on which the tool executes, wherein the tool definition specifies roles associated with the tool via an authorization model, and wherein a user assigned with one or more of the roles can run the tool on the target nodes;

extracting from the tool definition the roles associated with a the tool;

checking if any of the roles associated with the tool are enabled;

checking if the user has authorization on the target nodes; and

checking if the user is assigned with at least one of the enabled roles on all of the target nodes, wherein the user is authorized to run a requested tool if the user is assigned with one or more of the enabled roles associated with the requested tool on all of the target nodes.

2. (previously presented): The computer implemented method of claim 1, wherein the obtaining the roles step includes obtaining the roles associated with the tool, wherein the tool may be assigned one or more roles.

3. (previously presented): The computer implemented method of claim 1, further comprising validating the roles.

4. (previously presented): The computer implemented method of claim 1, further comprising obtaining the user's authorized roles for each node in the list of target nodes from a hash table.

5. (previously presented): The computer implemented method of claim 1, further comprising reporting whether the tool is runnable by the user.

6. (previously presented): The computer implemented method of claim 5, wherein the reporting step includes reporting the tool as not runnable by the user when all the roles are disabled.

7. (previously presented): The computer implemented method of claim 5, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized on each of the nodes.

8. (previously presented): The computer implemented method of claim 5, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized for any of the enabled roles on all of the nodes.

9. (previously presented): A service control manager (SCM) module implemented by a computer for validating a user's authorization to run a tool on one or more target nodes, comprising:

target nodes that are managed servers;

tools that specify commands or options on the target nodes, each tool including a tool definition, wherein the tool definition specifies roles associated with a tool via an authorization model;

roles associated with a tool, wherein a user assigned with one or more of the roles can run the tool on the target nodes; and

a security manager that checks whether any of the roles associated with the tool is enabled, and whether the user is assigned with one of the enabled roles on all of the target nodes, wherein the user is authorized to run a requested tool if the user is assigned with one or more of the enabled roles associated with the requested tool on all of the target nodes.

10. (original): The SCM module of claim 9, wherein the tools are single-system aware (SSA) tools.

11. (original): The SCM module of claim 9, wherein the tools are multi-system aware (MSA) tools.

12. (original): The SCM module of claim 9, wherein the target nodes can be target node groups.

13. (previously presented): A computer implemented method for validating a user's authorization to run a tool in a service control manager (SCM) module by a security manager, comprising:

creating a runnable tool, wherein the runnable tool encapsulates a tool and includes a tool definition and a list of target nodes on which the tool executes, wherein the tool definition specifies roles associated with a the tool via an authorization model, and wherein a user assigned with one or more of the roles can run the tool on the target nodes;

extracting from the tool definition the roles associated with a the tool;

checking if any of the roles associated with the tool are enabled; and

checking if the user is assigned with one of the roles associated with the tool on all of the target nodes, wherein the user is authorized to run a requested tool if the user is assigned with one of the roles associated with the requested tool on all of the target nodes.

14. (previously presented): The computer implemented method of claim 13, wherein the obtaining the roles step includes obtaining the roles associated with the tool, wherein the tool may be assigned one or more roles.

15. (previously presented): The computer implemented method of claim 13, further comprising validating the roles.

16. (previously presented): The computer implemented method of claim 13, further comprising obtaining the user's authorized roles for each node in the list of target nodes from a hash table.

17. (previously presented): The computer implemented method of claim 13, further comprising reporting whether the tool is runnable by the user.

18. (previously presented): The computer implemented method of claim 17, wherein the reporting step includes reporting the tool as not runnable by the user when all the roles are disabled.

19. (previously presented): The computer implemented method of claim 17, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized on each of the nodes.

20. (previously presented): The computer implemented method of claim 17, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized for any of the enabled roles on all of the nodes.